WHAT IS CLAIMED:

1. A method of enabling the use of a first digital work on plural computing devices, said method comprising the acts of:

receiving, from a first computing device, a user's credentials;

5   authenticating said credentials by querying a namespace authority;

providing a first activation certificate to said first computing device; and

persisting an association between said credentials and at least some information included in said first activation certificate.

10

2. The method of claim 1, wherein said computing device stores software having an activated state and a non-activated state, wherein said first activation certificate transforms said software to said activated state, wherein said software renders a second digital work regardless of whether it is in the activated state, and wherein said software renders said

15   first digital work only if said software is in the activated state.

3. The method of claim 1, wherein said first activation certificate comprises first data indicative of said user.

20   4. The method of claim 1, wherein said first activation certificate comprises a first cryptographic key, and wherein said first digital work comprises at least some data requiring said first cryptographic key for its use.

5. The method of claim 4, wherein the at least some information persistently

25   associated with said credentials comprises said first cryptographic key.

6. The method of claim 4, wherein said first digital work comprises encrypted content and a decryption key which decrypts said encrypted content, said decryption key

being included in said first digital work in an encrypted or sealed form decryptable or unsealable by said first cryptographic key.

7. The method of claim 5, wherein said first activation certificate further comprises a second cryptographic key, wherein said first and second cryptographic keys are the private and public keys, respectively, of an asymmetric key pair, and wherein said decryption key is included in said first digital work in a form encrypted by said second cryptographic key.

8. The method of claim 1, wherein said credentials comprise a username and a password.

9. The method of claim 1, further comprising the acts of:
        receiving, from a second computing device, said credentials;
        accessing the persisted information associated with said credentials;
        providing, to said second computing device, a second activation certificate based at least in part on the persisted information.

10. The method of claim 1, further comprising the acts of:
        receiving, from a second computing device, said credentials;
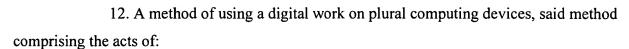   determining whether a first limit has been reached; and
        if said first limit has not been reached, providing to said second computing device a second activation certificate based at least in part on the persisted information associated with said credentials.

11. A computer-readable medium having computer-executable instructions to perform the method of claim 1.

12. A method of using a digital work on plural computing devices, said method comprising the acts of:

on a first computing device, transmitting credentials to an activation arrangement;

5   receiving, from said activation arrangement, a first activation certificate comprising a first cryptographic key;

on a second computing device, transmitting said credentials to said activation arrangement; and

receiving, from said activation arrangement, a second activation

10   certificate comprising said first cryptographic key;

wherein said digital work requires said first cryptographic key for its proper use.

13. The method of claim 12, wherein said credentials comprise a username and a password.

15

14. The method of claim 12, further comprising the act of authenticating said credentials.

15. The method of claim 12, wherein said first cryptographic key is included in

20   said first activation certificate in a first form, and wherein said first cryptographic key is included in said second activation certificate in a second form different from said first form.

16. The method of claim 12, wherein said activation arrangement comprises one or more server computing devices.

25

17. The method of claim 12, wherein said digital work comprises encrypted content and a second cryptographic key which decrypts said encrypted content, said second cryptographic key being included in said digital work in an encrypted form decryptable by said first cryptographic key.

18. The method of claim 12, further comprising the acts of:

transmitting, to a content provider, at least some information included in said first activation certificate; and

5   receiving, from said content provider, said digital work.

19. The method of claim 12, wherein said first activation certificate is at least partly resistant to being used on a computing device other than said first computing device, and wherein said second activation certificate is at least partly resistant to being used on a

10   computing device other than said second computing device.

20. The method of claim 12, wherein each of said first and second activation certificates includes information indicative of said credentials.

15   21. A method of enabling the use of an item on plural computing devices, said method comprising the act of:

providing, to a first computing device associated with a persona, first data which enables the use of said item on said first computing device; and

determining that a second computing device is associated with said

20   persona; and

providing to said second computing device second data which enables the use of said item on said second computing device.

22. The method of claim 21, wherein said item comprises digital content, and

25   wherein use of said item comprises rendering said digital content.

23. The method of claim 22, wherein said digital content comprises textual content, and wherein use of said item comprises displaying said textual content on a viewing device.

24. The method of claim 22, wherein said digital content comprises multimedia content, and wherein use of said item comprises rendering said multimedia content on a device adapted to render said multimedia content.

5

25. The method of claim 21, further comprising the acts of:

receiving, from said first computing device, third data indicative of said persona; and

prior to providing said first data to said computing device, 10 authenticating said third data.

26. The method of claim 25, wherein said third data comprises a username and a password, and wherein said authenticating act comprises querying a namespace authority as to the validity of said username and said password.

15

27. The method of claim 21, wherein said first data differs in at least some respect from said second data.

28. The method of claim 27, wherein said first data comprises a first 20 cryptographic key which enables the use of said item, said first cryptographic key being included in said first data in a form encrypted by a second cryptographic key, and wherein said second data comprises said first cryptographic key in a form encrypted by a third cryptographic key different from said second cryptographic key.

25   29. The method of claim 28, wherein said item comprises encrypted content and a decryption key which decrypts said encrypted content, and wherein said decryption key is encrypted so as to be decryptable by said first cryptographic key.

30. The method of claim 29, wherein said first data further comprises a fourth cryptographic key, wherein said second data further comprises said fourth cryptographic key, wherein said first and fourth cryptographic keys are the private and public keys, respectively, of an asymmetric key pair, and wherein said decryption key is included in said item in a form

5 encrypted by said fourth cryptographic key.

31. The method of claim 30, further comprising the acts of:

providing to said first computing device a first set of computer-executable instructions which applies said second cryptographic key; and

10 providing to said second computing device a second set of computer-executable instructions which applies said third cryptographic key.

32. The method of claim 27, further comprising the act of persisting an association between said persona and at least some of said first data.

15

33. The method of claim 21, wherein said item does not reside on said first computing device at the time said first data is provided to said first computing device.

34. The method of claim 33, wherein said item is created subsequent to the acts

20 of providing said first and second data to said first and second computing devices respectively.

35. The method of claim 21, further comprising the act of determining the number of computing devices on which use of said item is enabled.

25

36. The method of claim 21, further comprising the act of determining, prior to providing said second data to said second computing device, the amount of time that has elapsed since use of said item was enabled on said first computing device.

37. The method of claim 21, wherein said first and second data each include information indicative of said persona.

38. A computer-readable medium having computer-executable instructions to
5   perform the method of claim 21.

39. A method of activating software on a remote computing device for use by an individual user, the method comprising:
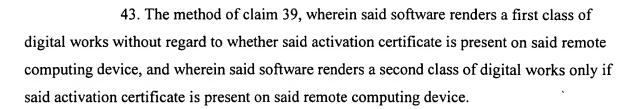
        receiving the individual user's credentials;

10   authenticating the individual user's credentials by querying a namespace authority;

        requesting first information from the remote computing device;

        generating an activation certificate that includes second information related to the user's credentials; and

15   downloading said activation certificate to the remote computing device to activate the software residing on the remote computing device such that at least some aspect of operation of the software is associated with the individual user's credentials.

40. The method of claim 39, wherein said first information is based on or
20   identifies at least some hardware associated with said remote computing device.

41. The method of claim 39, wherein said activation includes at least some resistance to being used on a computing device different from said remote computing device.

25   42. The method of claim 41, wherein said activation certificate further includes the public and private keys of an asymmetric key pair, said private key being included in said activation certificate in a form encrypted by a first cryptographic key.

43. The method of claim 39, wherein said software renders a first class of digital works without regard to whether said activation certificate is present on said remote computing device, and wherein said software renders a second class of digital works only if said activation certificate is present on said remote computing device.

5

44. A computer-readable medium having computer-executable instructions to perform the method of claim 39.